Американска стопанска комора
Северна Македонија

Дополнителни препораки во однос на Нацрт-Закон за безбедност на мрежни и информациски системи

Скопје, март 2025

I. Опфат на Законот: Потенцијална прекумерна регулација

Постои загриженост дека нацрт-Законот може да има поширок опфат од предвидениот во Директивата на ЕУ 2022/2555 (NIS 2) во однос на барањата и обврските. Идентификуваме три клучни точки каде што постои ризик од прекумерна регулација:

Прва точка

Нацрт- Закон за безбедност на мрежни и информациски системи (одредби)	Директива на ЕУ 2022/2555 (NIS 2) (одредби)
Со член 4 став (2) од Нацрт-Законот се уредува дека Законот се применува на работата на средни и големи субјекти кои обезбедуваат услуги во дефинираните сектори (вкупно 16 сектори). Притоа, не се прави разлика на сектори со висока критичност и други критични сектори.	Со член 2 став (1) од Директивата, се уредува дека истата се применува на видовите на субјекти наведени во Анекс I или II, кои се квалификуваат како средни претпријатија или големи претпријатија. Во Анекс 1 се дефинирани секторите со висока критичност (Annex I: Sectors of high criticality), а во Анекс II се дефинирани другите критични сектори (Annex II: Other critical sectors). „Article 2 Scope 1. This Directive applies to public or private entities of a type referred to in Annex I or II which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC,or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, and which provide their services or carry out their activities within the Union.”
Во член 8 став (1) точка 1 од Законот се уредува дека суштински субјекти се големите субјекти кои припаѓаат на секторите од член 4 став (2), односно сите големи субјекти кои обезбедуваат во овие 16 сектори.	Членот 3 став (1) точка а) уредува дека суштински субјекти се субјектите наведен во Анекс I, кои ги надминуваат праговите за средни претпријатија, односно големите субјекти. „1. For the purposes of this Directive, the following entities shall be considered to be essential entities: (a) entities of a type referred to in Annex I which exceed the

	ceilings for medium-sized enterprises provided for in Article 2(1) of the Annex to Recommendation 2003/361/EC”

Иако член 7 од нацрт-Законот предвидува соодветна дистинкција помеѓу: (1) сектори со висока критичност и (2) други критични сектори преку подзаконските акти и деталните листи, набројувањето на секторите во член 4 став (2), без категоризација на високо критични и други критични сектори доведува до прекумерна регулација.
Имено, согласно член 8 став (1) точка 1 од нацрт - Законот, големите субјекти кои припаѓаат на категоријата (2) – други критични сектори, како што се производство, преработка и дистрибуција на храна, индустриско производство и други, ќе бидат класифицирани како суштински субјекти. Сепак, согласно Директивата, овие големи субјекти треба да бидат класифицирани како важни субјекти. Ваквото уредување со нацрт - Законот би значело наметнување дополнителни обврски кои го надминуваат предвиденото во Директивата на ЕУ, што би резултирало со прекумерна регулација за засегнатите субјекти во државата.
Затоа, предлагаме да се направи јасна дистинкција при класификацијата на субјектите, врз основа на тоа дали припаѓаат на сектори со висока критичност или на други критични сектори, во согласност со директивата.

Втора точка

Нацрт- Закон за безбедност на мрежни и информациски системи (одредби)	Директива на ЕУ 2022/2555 (NIS 2) (одредби)
Со член 4 став (3) од Законот се уредува дека одредбите на овој закон се применуваат на сите правни лица со регистрирано седиште во Републиката, независно од нивната големина, доколку ги исполнуваат услови наведени во точки 1 – 7.	Со членот 2 од Директивата се уредува дека, независно од нивната големина, оваа директивата се применува на сите субјекти од видовите наведени во Анекс I или II, доколку ги исполнуваат услови наведени во точки а – ѓ. „Regardless of their size, this Directive also applies to entities of a type referred to in Annex I or II, where:..”

Потенцијалната прекумерната регулација може да се јави во врска со точка 5 од став (3), член 4 од нацрт - Законот, кој пропишува дека обврските од Законот ќе се применуваат и доколку правното лице, поради својата посебна важност, се смета за критично за одреден сектор или тип на услуга.
Ова значи дека субјект кој е критично важен за својот сектор, дури и ако тој сектор не е наведен во член 4 став (2) од нацрт - Законот, ниту е опфатен со деталните

листи на потсектори и видови на субјекти, сепак може да биде класифициран како важен субјект. Постојат примери во производството на пиво, обработката на тутун и други индустрии, каде што одредени субјекти потенцијално го исполнуваат критериумот од точка 5 во член 4 став (3).

Ако оваа одредба од нацрт - Законот не биде прецизно ограничена на видовите субјекти од веќе дефинираните сектори и потсектори, тоа може да доведе до наметнување на обврски на субјекти кои, согласно Директивата, не би требало да бидат опфатени.
Дополнително, покрај тоа што негативно ќе влијае на конкурентноста на овие субјекти, ваквата регулаторна пракса ќе предизвика и неоправдано трошење на ресурсите на страната на надзорните органи.

Затоа, предлагаме ставот (3) од член 4 да се однесува само на видовите субјекти од веќе дефинираните сектори и потсектори, со цел да се обезбеди усогласеност со ЕУ регулативите.

Трета точка

Нацрт- Закон за безбедност на мрежни и информациски системи (одредби)	Директива на ЕУ 2022/2555 (NIS 2) (одредби)
Со член 9 став (1) точки 11 и 12 се уредува дека даватели на услуги на суштински субјекти и важни субјекти кои што немаат регистрирано седиште во Републиката, имаат должност да регистрираат свој претставник во MKD-CIRT.	Со членот 26 став (3) од директивата се уредува дека доколку субјектот наведен во став 1, точка (б), не е основан во Унијата, но нуди услуги во рамките на Унијата, тој треба да назначи претставник во Унијата. Став (1) точка б од истиот член на Директивата се однесува на субјектите наведени во точки 1-10, односно не се однесува и на давателите на услуги на суштинските и важните субјекти: „b) DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines or of social networking services platforms, which shall

	be considered to fall under the jurisdiction of the Member State in which they have their main establishment in the Union under paragraph 2;"
Во дефиницијата бр. 43 со која што се уредува што значи претставник, не се наведени точките 11 и 12, односно се однесува само на точките 1-10: 43) „**претставник**" е физичко или правно лице кое е изречно назначено да делува во име на давател на услуги за DNS, регистар на имиња на врвни домени, субјект/давател на услуги за регистрација на имиња на домени, давател на услуги за компјутерска обработка во облак, давател на услуги за податочен центар, давател на услуги за мрежи за испорака на содржини, давател на управувани услуги, давател на управувани безбедносни услуги, давател на услуга на интернет-пазар, давател на услуги на пребарувачи на интернет или давател на платформи за услуги за социјални мрежи што нема регистрирано седиште во Република Северна Македонија и до кое може да се обрати Министерството за дигитална трансформација во однос на обврските на тој субјект што произлегуваат од овој закон;	Дефиницијата од нацрт - Законот е целосно усогласена со дефиниција за претставник од Директивата на ЕУ, односно со член 6 точка 34: „(34) 'representative' means a natural or legal person established in the Union explicitly designated to act on behalf of a DNS service provider, a TLD name registry, an entity providing domain name registration services, a cloud computing service provider, a data centre service provider, a content delivery network provider, a managed service provider, a managed security service provider, or a provider of an online marketplace, of an online search engine or of a social networking services platform that is not established in the Union, which may be addressed by a competent authority or a CSIRT in the place of the entity itself with regard to the obligations of that entity under this Directive;"

Воведувањето на обврска за регистрација на претставник во MKD-CIRT за давателите на услуги на суштински и важни субјекти кои немаат регистрирано седиште во Републиката, исто така не е предвидено со Директивата.

Директивата веќе осигурува дека суштинските и важните субјекти се одговорни за мерките за сајбер безбедност. Оттука, воведувањето на дополнителна регистрација за давателите на услуги на овие субјекти не ја зголемува безбедноста, туку создава непотребни административни компликации за бизнисите. Впрочем, ова може да доведе до пречки за компаниите што во Северна Македонија нудат услуги што не се критични, потенцијално обесхрабрувајќи го нивното учество на пазарот. Ова, пак, може да има негативни последици врз квалитетот на услугите и конкурентноста на пазарот.

Затоа, предлагаме точките точки 11 и 12 од став (1) на член 9 да се избришат.

Дополнително, треба соодветно да се ревидираат податоците за регистрацијата согласно член 9, став (3), односно да се има предвид дека претставник може да биде и правно лице, при што точката 3) не би била применлива.

II. Дополнителни предлози

Примена на програми и стандарди

Одредбите кои се однесуваат на примена на европски и меѓународни програми за сајбер безбедносна сертификација (член 35) и стандарди за безбедност на мрежни и информациски системи (член 36) предвидено е да започнат да се применуваат од денот на пристапување во ЕУ.

Оставањето можност субјектите на кои се однесува нацрт-Законот, вклучително и јавните институции да набавуваат и користат ИКТ производи, системи и услуги кои не задоволуваат соодветни ЕУ и меѓународни стандарди за сајбер безбедност во периодот до пристапувањето во ЕУ може да резултира со последици што се дијаметрално спротивни од целите на овој Закон.

Од овие причини, предлагаме примената на членовите 35 и 36 да започне со примената на Законот, а не од денот на пристапување во ЕУ. Единствено на тој начин е можна изградба на капацитетите за безбедност на мрежни и информациски системи во државата.

Организациската структура за сајбер безбедност

Согласно член 8 став (6) од нацрт - Законот, суштинските субјекти, односно големите компании што припаѓаат на одредените сектори, во зависност од нивната големина и обемот на работа, се должни: или да формираат организациска единица за сајбер-безбедност, или да овластат најмалку едно лице како офицер за сајбер-безбедност. Конкретните критериуми во однос на големината и обемот на работа за формирање на организациска единица ќе ги утврдува министерот со подзаконски акт.

Ставови (1) и (2) на член 25 од нацрт - Законот пропишуваат дека институциите од јавниот сектор се должни да систематизираат и пополнат работно место за офицер за сајбер безбедност или да формираат посебна организациска единица, а останатите суштински субјекти, вклучително и големите компании што припаѓаат на

соодветно дефинираните сектори, се должни да имаат вработено или на друг начин ангажирано офицер за сајбер безбедност.

Врз основа на овие одредби, не е јасно која обврска конкретно се однесува на големите субјекти од дефинираните сектори. Затоа, предлагаме во член 8 став (6) точка 1) да се замени со точка 4), со цел да се постигне поголема правна прецизност.

Наметнувањето на обврска за големите компании, особено за мултинационалните, да формираат специјализирана единица за сајбер-безбедност врз основа на подзаконски акт што го дефинира нивниот обем на работа и големина, е проблематично од правен, практичен и економски аспект.

Уредување на прекршочните одредби

Со член 51 се уредува дека на клучните субјекти ќе им се изрекува глоба во износ до 2% од нивниот вкупен годишен приход. Иако ваквото уредување е во согласност со одредбите од Законот за прекршоците, а споменатиот процент е во согласност со Директивата (ЕУ) 2022/2555 (НИС 2), веруваме дека треба да се земе предвид и фактот дека со овој закон за првпат се воспоставува сеопфатна регулатива за безбедноста на мрежните и информациските системи во нашата држава. ЕУ Директивата 2016/1148 (НИС 1) од 2016 година, не содржи вакви одредби. Наместо тоа, беше оставен простор на поединечните земји-членки самите да ги дефинираат висините на глобите, со цел глобите да бидат прилагодени на економските капацитети на компаниите во различни земји. На овој начин, компаниите во ЕУ имаа време да се запознаат со новите обврски за сајбер безбедност и да ги прилагодат нивните внатрешни процеси пред да се премине кон уредување на минималниот износ на највисоката глоба што може да се изрече.

Имајќи предвид дека најголем дел од клучните субјекти кај нас би биле средни компании, под претпоставка дека нивната големина се утврдува според Законот за трговските друштва, нивниот годишен приход би бил помеѓу 2 и 10 милиони евра. Ова значи дека казната за нив би изнесувала потенцијално до 200.000 евра. Висината на овие износи не само што би можела да создаде сериозен финансиски притисок за компаниите, туку и да го загрози нивното постоење.

Од овие причини, предлагаме да се усвои фазен пристап во времетраење од минимум пет години, започнувајќи со пониски глоби и постепено зголемување на прагот. На пример, да се започне со 0,3% за првата година, а да се достигнат 2% во период од минимум пет години или со официјално зачленување во Европската Унија. Со ова би се обезбедило доволно време за компаниите да ги разберат новите барања и да се усогласат со нив и би се избегнал регулаторен шок кој би можел сериозно да влијае врз нивното деловно работење.

Почеток на примена на законот

Предлагаме примената на законот за сите субјекти да започне 12 месеци по усвојувањето на подзаконските акти. Откако ќе се изготват деталните листи на потсектори и видови на субјекти, врз основа на кои ќе се утврдат листите на суштински и важни субјекти, засегнатите субјекти ќе имаат јасна претстава дека треба да започнат со подготовка за обврските што произлегуваат од овој закон. Оваа подготовка, вклучувајќи го и финансиското планирање, не може да биде пократка од 12 месеци.